การวิเคราะห์การนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ

The Analysis of the Implementation of the Computer–Related Crime Act B.E. 2550

[1]**วรพิทย์ มีมาก (Worapit Meemak)**
[2]**ประพีร์ อภิชาติสกล (Prapee Apichatsakol)**
มหาวิทยาลัยศรีนครินทรวิโรฒ (Srinakarinwirot University)
E–mail: vorapitaya@hotmail.com

Received January 21, 2020; **Revised** February 10, 2020; **Accepted** February 25, 2020

Abstract

This research aimed to analyze and identify factors affecting the implementation of the Computer–Related Crime Act B.E. 2550. Samples composed of 30 relevant officials under Ministry of Digital Economy and Society, Royal Thai Police, and Department of Special Investigation, and 70 public and private Internet operators. Data collected through a reliability–tested questionnaire were analyzed via analysis of variance, analysis of covariance, and multiple regression analysis. The findings indicated that legal implementation by the authorized persons was effective at a moderate level, and factors affecting legal implementation were implementers' behavior and legal entity structure.

Keywords: Legal implementation, Computer act, Computer–related crime

บทคัดย่อ

งานวิจัยฉบับนี้มีวัตถุประสงค์เพื่อ วิเคราะห์ผลลัพธ์และระบุปัจจัยที่ส่งผลต่อการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ กลุ่มตัวอย่าง ได้แก่ พนักงานเจ้าหน้าที่ของรัฐที่เกี่ยวข้องซึ่งสังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ จำนวน 30 คน และผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐและในหน่วยงานภาคเอกชน จำนวน 70 คน เครื่องมือการวิจัย ได้แก่ แบบสอบถามที่ผ่านการทดสอบความเชื่อถือได้ สถิติวิจัยใช้การวิเคราะห์ความแปรปรวน การวิเคราะห์ความแปรปรวนร่วม และการวิเคราะห์ถดถอยพหุ ผลการวิจัยพบว่า การนำกฎหมายไปปฏิบัติได้ผลในระดับปานกลาง ส่วนปัจจัยที่ส่งผลต่อการนำกฎหมายไปปฏิบัติ ได้แก่ พฤติกรรมของผู้ปฏิบัติงาน และโครงสร้างของหน่วยงานตามกฎหมาย

คำสำคัญ: การนำกฎหมายไปปฏิบัติ, กฎหมายคอมพิวเตอร์, การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

บทนำ

ปัจจุบันระบบคอมพิวเตอร์ได้เข้ามามีบทบาทอย่างมากในวิถีชีวิตของมนุษย์ ทั้งในเรื่องเฉพาะบุคคล กลุ่มองค์การ และสังคม ดังนั้น ถ้ามีผู้กระทำด้วยประการใด ๆ ที่อาจจะก่อความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจจะเป็นได้ในรูปแบบของการเผยแพร่ข้อมูลคอมพิวเตอร์ปลอม/ ข้อมูลคอมพิวเตอร์อันเป็นเท็จ การทำลาย แก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ก็จะส่งผลกระทบทางลบตามมาอย่างมาก ในแง่ผลต่อบุคคล กลุ่ม และองค์การจะเป็นเรื่องของการเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ส่วนผลต่อส่วนรวม คือ จะทำให้เกิดความเสียหายเกี่ยวกับความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ รวมไปถึงความสงบสุขและศีลธรรมอันดีของประชาชน ซึ่งผลกระทบต่อส่วนรวมจะก่อความเสียหายอย่างมหาศาล ดังนั้นเพื่อป้องกันผลในทางลบ กลไกสำคัญที่รัฐนำมาใช้ คือ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เจตนารมณ์พื้นฐานของกฎหมายดังกล่าว ได้แก่ การป้องกันและปราบปรามอาชญากรรมที่เกิดจากคอมพิวเตอร์โดยตรง ซึ่งไม่สามารถใช้บทบัญญัติในประมวลกฎหมายอาญามาบังคับใช้ได้ เพราะมีองค์ประกอบของความผิดแตกต่างกัน อย่างไรก็ตาม ในทางปฏิบัติ ปัญหาสำคัญ ที่พบได้นับตั้งแต่กฎหมายฉบับนี้มีผลบังคับใช้ ได้แก่ (Napibul, 2008) (1) ความไม่ชัดเจนของบทบัญญัติแห่งกฎหมายทำให้เกิดปัญหาในการตีความ (2) ความไม่ครอบคลุมของบทบัญญัติแห่งกฎหมาย การกระทำที่เกิดขึ้นบางกรณียังไม่มีบทบัญญัติแห่งกฎหมายกำหนดให้เป็นความผิด และ (3) ปัญหาเกี่ยวกับบทกำหนดโทษ อนึ่ง หลังจาก พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ใช้มา 10 ปี ก็ได้มีการแก้ไขเพิ่มเติมเป็น พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ทั้งนี้เพื่อให้สอดคล้องกับยุคสมัย และปรับหลักเกณฑ์ รวมทั้งอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น อย่างไรก็ตาม ยังมีข้อกังขาว่า กฎหมายฉบับปรับปรุงอาจไม่ต่างไปจากฉบับเดิม เพราะอาจถูกนำมาใช้ตั้งข้อหาหมิ่นประมาทและความมั่นคง รวมไปถึงการดำเนินคดีกับผู้เรียกร้องสิทธิเสรีภาพ แสดงความเห็นทางการเมือง และปกป้องสิทธิมนุษยชน ในลักษณะที่เรียกว่า ‘ฟ้องปิดปาก’ มากกว่าที่จะนำมาใช้ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนั้น ประเด็นที่น่าสนใจศึกษา คือ ผลลัพธ์ที่เกิดขึ้นหลังจากการปรับปรุงกฎหมายเป็นอย่างไร

โดยเฉพาะในแง่ของการให้หลักประกันเกี่ยวกับสิทธิเสรีภาพในเรื่องของการให้บริการและการใช้บริการคอมพิวเตอร์ รวมไปถึงความเชื่อมั่นของประชาชนจากการบังคับใช้กฎหมาย และมีปัจจัยใดบ้างที่เข้ามาส่งผลกระทบต่อการนำกฎหมายไปปฏิบัติ ซึ่งประเด็นดังกล่าวถือว่ามีความสำคัญเป็นอย่างยิ่งต่อการบ่งชี้ประสิทธิผลของกฎหมาย

วัตถุประสงค์การวิจัย

1. เพื่อวิเคราะห์ผลลัพธ์จากการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ

2. เพื่อเปรียบเทียบทัศนะระหว่างพนักงานเจ้าหน้าที่ ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

3. เพื่อระบุปัจจัยที่ส่งผลต่อการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ

ขอบเขตของการวิจัย

ขอบเขตด้านเนื้อหา ใช้การผสมผสานแนวคิดการนำนโยบายไปปฏิบัติของนักวิชาการที่ศึกษาเกี่ยวกับการนำนโยบายไปปฏิบัติ โดยมีตัวแปรที่ใช้ในการศึกษา ดังนี้ ตัวแปรตาม ได้แก่ ผลลัพธ์ที่เกิดขึ้นจากการนำ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ ตัวแปรอิสระ ได้แก่ เจตนารมณ์ของกฎหมาย โครงสร้างของหน่วยงานตามกฎหมาย มาตรฐานของกฎหมาย คุณสมบัติของผู้ปฏิบัติงาน การประสานงาน ความชัดเจนของกฎหมาย พฤติกรรมของผู้ปฏิบัติงานและเงื่อนไขทางเศรษฐกิจ สังคม และการเมือง

ขอบเขตด้านประชากรและการสุ่มตัวอย่าง ประชากร ได้แก่ (1) พนักงานเจ้าหน้าที่ของรัฐที่เกี่ยวข้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ และ (2) ผู้ดำเนินการอินเทอร์เน็ตที่เกี่ยวข้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในหน่วยงานภาครัฐและภาคเอกชน โดยจะสุ่มตัวอย่างแบบชั้นภูมิเชิงสัดส่วน (Proportional stratified random sampling) จากกลุ่ม (1) และ (2) จำนวน 30 คน และ 70 คน ตามลำดับ

ทบทวนวรรณกรรม

นิยามศัพท์

การนำนโยบายไปปฏิบัติ หมายถึง การกระทำกิจกรรมต่าง ๆ ให้เกิดขึ้นอย่างต่อเนื่องในความสัมพันธ์เชิงเหตุผล โดยหน่วยผลิตภาครัฐหรือภาคเอกชนตามการตัดสินใจเชิงนโยบายของนักการเมืองหรือผู้บริหารระดับสูง เพื่อการบรรลุผลสัมฤทธิ์ตามเป้าหมายที่ได้กำหนดไว้ (Pressman, & Wildavsky, 1973; Van Meter, & Van Horn, 1975; Mazmanian, & Sabatier, 1983)

อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำความผิดใด ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์และ/หรือเครือข่ายอาทิ อินเทอร์เน็ต โทรศัพท์เคลื่อนที่ ฯลฯ ทั้งนี้เพื่อแสวงหาผลประโยชน์โดยมิชอบ ซึ่งมีขอบเขตตั้งแต่บุคคลไปกระทั่งถึง

ประเทศในแง่ของบุคคลอาจเกี่ยวข้องกับการทำร้ายร่างกายหรือจิตใจของผู้ถูกกระทำ การนำข้อมูลทางธุรกิจของผู้อื่นมาเปิดเผยทางอินเทอร์เน็ตโดยไม่ได้รับอนุญาต การขโมยข้อมูลส่วนบุคคล การละเมิดเสรีภาพโดยการลักลอบใช้คอมพิวเตอร์ของบุคคลอื่น เป็นต้น ในแง่ของประเทศอาจมุ่งก่อการร้าย ทำลายระบบการเงิน ฯลฯ (Moore, 2005; Brenner, 2012; Hill, & Marion, 2016)

แนวคิด /ทฤษฎี

การนำนโยบายไปปฏิบัติ แนวคิดที่เกี่ยวข้องกับการนำนโยบายไปปฏิบัติสามารถจำแนกได้เป็น 3 แนวคิด ได้แก่ (1) แนวคิดที่ให้ความสำคัญต่อฝ่ายบริหาร (Top down approach) แนวคิดนี้เน้นในเรื่องการตัดสินใจของฝ่ายบริหารและการออกแบบนโยบายที่สมเหตุสมผล การพัฒนาข้อแนะนำเชิงนโยบายที่สามารถนำไปใช้ได้เป็นการทั่วไป (Schofield, 2001) (2) แนวคิดที่ให้ความสำคัญต่อฝ่ายปฏิบัติ (Bottom up approach) แนวคิดนี้มุ่งเน้นบทบาทและพฤติกรรมของผู้ปฏิบัติ โดยการสังเกตข้อเท็จจริงของพฤติกรรมที่เกิดขึ้นจากการนำนโยบายไปปฏิบัติ ด้วยการตอบคำถามว่าทำไม (Why) และอย่างไร (How) รวมไปถึงการค้นหาความสัมพันธ์ระหว่างพฤติกรรมที่เกิดขึ้นกับนโยบายนั้น (Barrett, & Fudge (Eds.), 1981; Schofield, 2001) และ (3) แนวคิดเชิงผสมผสาน (Hybrid approach) Goggin, Bowman, Lester, & O'Toole, Jr. (1990) เสนอตัวแบบการสื่อสาร โดยให้ทั้งส่วนกลางและส่วนปฏิบัติ สื่อสารเกี่ยวกับแรงจูงใจที่จะให้และเงื่อนไขข้อจำกัดที่ควรตระหนัก รวมไปถึงผลลัพธ์จากการตัดสินใจและสมรรถนะในการดำเนินงาน การสื่อสารจากทั้งส่วนกลางและส่วนปฏิบัติ จะเป็นการส่งสัญญาณให้เห็นถึงความเหมือนและความแตกต่างของการรับรู้ ซึ่งจะนำไปสู่การปรับปรุงแก้ไขต่อไป Sabatier (1991) เสนอให้มีการเรียนรู้เชิงนโยบายเกิดขึ้นทั้งในระดับบริหารและปฏิบัติการ กล่าวคือ ส่วนกลางจะต้องใช้เวลาในการวิเคราะห์วงจรนโยบายที่ยาวนานขึ้น ขณะเดียวกันก็เปิดโอกาสให้กลุ่มต่าง ๆ ได้เข้ามามีส่วนร่วมในนโยบายมากขึ้น ซึ่งนอกจากจะทำให้เกิดมุมมองที่หลากหลายแล้ว ยังจะทำให้เกิดความชอบธรรมและการยอมรับนโยบายนั้นมากขึ้นด้วย อนึ่งเพื่อให้การนำนโยบายไปปฏิบัติสามารถบรรลุผลได้ตามวัตถุประสงค์ที่กำหนดไว้ Nakamura, & Smallwood (1980) ได้เสนอให้ใช้เกณฑ์การวัดผลลัพธ์ ของการนำนโยบายไปปฏิบัติ 5 ประการ ดังนี้ (1) การเปรียบเทียบผลลัพธ์ที่ได้จากการปฏิบัติงานกับเป้าหมายที่กำหนดไว้ (2) การสนับสนุนหรือการคัดค้านนโยบาย (3) การตอบสนองความต้องการของประชาชน (4) ประสิทธิภาพ และ (5) การธำรงรักษาระบบ

สำหรับปัจจัยที่ส่งผลต่อการนำนโยบายไปปฏิบัตินั้น Van Meter, & Van Horn (1975) ระบุว่ามี 6 ตัวแปร ได้แก่ มาตรฐานและวัตถุประสงค์ของนโยบาย ทรัพยากรที่นำมาใช้ การสื่อสารระหว่างองค์การและกิจกรรมการปฏิบัติ ลักษณะของหน่วยปฏิบัติ ทัศนคติของผู้ปฏิบัติงาน และเงื่อนไขทางเศรษฐกิจ สังคมและการเมือง ส่วน Edwards III (1980) ได้เสนอตัวแบบปฏิสัมพันธ์ระหว่างปัจจัย 4 ปัจจัย ที่มีผลต่อการนำนโยบายไปปฏิบัติ ปัจจัยดังกล่าว ได้แก่ การติดต่อสื่อสาร ทรัพยากร ทัศนคติของฝ่ายปฏิบัติ และโครงสร้างของหน่วยงาน นอกจากนี้ ยังมีปัจจัยที่ส่งผลต่อการนำนโยบายไปปฏิบัติในทัศนะของนักวิชาการอื่น ๆ ดังนี้ การประสานงาน (Vangen, & Huxam, 2003) ลักษณะของนโยบาย (Ben-Zadok, 2006) ลักษณะของหน่วยงานที่นำนโยบายไปปฏิบัติ (Butler, 2003) พฤติกรรมของผู้ปฏิบัติงาน (Ryan, 1996) โครงสร้างขององค์การ (Terpstra, & Havinga, 2001)

อาชญากรรมคอมพิวเตอร์ การศึกษาคอมพิวเตอร์ในแง่มุมของอาชญากรรมมี 3 สถานะ ได้แก่ การเป็นตัวการ การเป็นวัตถุ และการเป็นเครื่องมือที่ใช้ในการทำความผิด (Parker, Nycum, & Oüra, 1973) ซึ่งความผิดที่เกิดขึ้นอาจ

เกี่ยวข้องกับเนื้อหา (Content) ข้อมูล (Data) ระบบ (Systems) เครือข่าย (Networks) และกระบวนการ (Processes) สำหรับทฤษฎีที่นำมาใช้อธิบายการก่ออาชญากรรมคอมพิวเตอร์จะมี อาทิ ทฤษฎีพันธะทางสังคม (Social bond theory) ทฤษฎีนี้อธิบายว่า บุคคลที่ยึดมั่นในเป้าหมายที่สังคมยอมรับ ปฏิบัติตนตามบรรทัดฐานและค่านิยมของสังคม สนใจสิ่งแวดล้อมทางสังคมและเข้าไปมีส่วนร่วมในกิจกรรมทางสังคม มีแนวโน้มที่จะกระทำผิดหรือต่อต้านสังคมน้อยกว่าบุคคลที่เปราะบาง (Vulnerable) (Hirschi, 1969) ทฤษฎีกิจกรรมปกติวิสัย (Routine activity theory) สาระสำคัญของทฤษฎี คือ การกระทำความผิดจะเกิดมาจากกิจวัตรที่บุคคลปฏิบัติเป็นประจำ ภายใต้เงื่อนไข 4 ประการ ได้แก่ แรงจูงใจ (Motivation) เป้าหมายที่เหมาะสม (Suitable target) ระดับของการพิทักษ์และการให้คำแนะนำ (Degree of protection and supervision) และโอกาส (Opportunity) (Cohen, & Felson, 1979) และทฤษฎีการเปลี่ยนผ่านเชิงพื้นที่ (Space transition theory) ซึ่งอธิบายว่าการก่ออาชญากรรมทั้งในพื้นที่ทางกายภาพและทางไซเบอร์สามารถถ่ายโอนซึ่งกันและกันได้ (Jaishankar, 2008)

งานวิจัยที่เกี่ยวข้อง ในประเทศไทยได้มีการศึกษาอาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในหลายแง่มุม อาทิ ความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ (Lertkitikul, 2007) ปัญหาและอุปสรรคที่ทำให้กฎหมายไม่สามารถบังคับใช้ได้อย่างมีประสิทธิภาพ (Na Pibul, 2008) ความรู้และพฤติกรรมการใช้อินเทอร์เน็ตที่เกี่ยวข้องกับกฎหมาย (Sakdulyatham, 2008) ความผิดเกี่ยวกับการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคงแห่งชาติ (Onpueng, 2011)

จากแนวคิด /ทฤษฎีและงานวิจัยที่เกี่ยวข้องดังกล่าวข้างต้น ตัวแปรที่คัดเลือกมาศึกษาจะได้แก่ เจตนารมณ์ของกฎหมาย โครงสร้างของหน่วยงานตามกฎหมาย มาตรฐานของกฎหมาย คุณสมบัติของผู้ปฏิบัติงาน การประสานงาน ความชัดเจนของกฎหมาย พฤติกรรมของผู้ปฏิบัติงาน และเงื่อนไขทางเศรษฐกิจ สังคม และการเมือง

วิธีดำเนินการวิจัย

ใช้การออกแบบการวิจัยเชิงสำรวจและวิธีการวิเคราะห์เชิงปริมาณสำหรับข้อมูลภาคตัดขวาง

1. ประชากรและการสุ่มตัวอย่าง ประชากร ได้แก่

(1) พนักงานเจ้าหน้าที่ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ

(2) ผู้ดำเนินการอินเทอร์เน็ตที่เกี่ยวข้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในหน่วยงานภาครัฐ (เช่น เจ้าของเว็บไซต์ ผู้ดูแลเว็บไซต์ ผู้ดูแลเว็บบอร์ด ผู้ให้บริการบล็อก ฯลฯ) และผู้ดำเนินการอินเทอร์เน็ต ที่เกี่ยวข้องกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในหน่วยงานภาคเอกชน (เช่น เจ้าของเว็บไซต์ ผู้ดูแลเว็บไซต์ ผู้ดูแลเว็บบอร์ด ผู้ให้บริการบล็อก เจ้าของร้านอินเทอร์เน็ต Network operator ผู้ให้บริการพื้นที่เก็บข้อมูลหรือโฮสต์ ผู้ประกอบการหอพัก/โรงแรม/ร้านอาหาร Internet service provider ฯลฯ)

การสุ่มตัวอย่าง จะสุ่มโดยใช้วิธีการสุ่มตัวอย่างแบบชั้นภูมิเชิงสัดส่วน (Proportional stratified random sampling) ขนาดของตัวอย่างคำนวณโดยใช้สูตรสัดส่วน ได้จำนวน 100 คน จำแนกเป็นกลุ่ม (1) และ (2) จำนวน 30 คน และ 70 คน ตามลำดับ

2. เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสอบถามที่ประมวลมาจากวรรณกรรมที่เกี่ยวข้อง และนำมาวิเคราะห์เพื่อสร้างแบบสอบถาม โดยใช้ Summated rating scale จำแนกเป็น 5 ระดับของ Likert และนำไปทดสอบหาความเชื่อถือได้ของแบบสอบถามที่สร้างขึ้นจากหน่วยงานภาคเอกชนที่เกี่ยวข้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในเขตกรุงเทพมหานคร จำนวน 30 คน โดยใช้ Cronbach's Alpha ผลการทดสอบได้ค่า Reliability Statistics เท่ากับ 0.902

3. การประมวลผลและการวิเคราะห์ข้อมูล กระทำโดย

(1) การวิเคราะห์ข้อมูลทั่วไปของกลุ่มตัวอย่าง ใช้สถิติพรรณนา (ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน)

(2) การวิเคราะห์ความแตกต่างของค่าเฉลี่ยความคิดเห็นของกลุ่มตัวอย่าง ใช้การวิเคราะห์ความแปรปรวน (Analysis of variance) และการวิเคราะห์ความแปรปรวนร่วม (Analysis of co-variance)

(3) การวิเคราะห์ปัจจัยที่ส่งผลต่อการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ ใช้การวิเคราะห์ถดถอยพหุ (Multiple regression analysis)

ผลการวิจัย

สมมติฐานและผลลัพธ์ที่ได้จากการทดสอบสมมติฐานมีดังนี้

สมมติฐานที่ 1 ผลลัพธ์ที่เกิดขึ้นจากการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ มีแนวโน้มที่จะประสบผลสำเร็จตามเจตนารมณ์ของกฎหมาย

ตารางที่ 1 ผลลัพธ์จากการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ จำแนกรายกลุ่ม

ผลลัพธ์ที่เกิดขึ้นจากการนำกฎหมายไปปฏิบัติ	$\bar{X}$	S.D.	การแปลผล
พนักงานเจ้าหน้าที่			
1. การตระหนักในการใช้คอมพิวเตอร์	4.367	0.718	เห็นด้วยอย่างยิ่ง
2. การป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์	3.700	0.837	ค่อนข้างเห็นด้วย
3. การป้องกันการละเมิดสิทธิเสรีภาพในการใช้คอมพิวเตอร์ของผู้อื่น	3.400	1.037	เห็นด้วยปานกลาง
4. การป้องกันการทำให้ระบบคอมพิวเตอร์ของผู้อื่นเสียหาย	3.067	1.285	เห็นด้วยปานกลาง
5. การใช้อำนาจของพนักงานเจ้าหน้าที่ที่กระทบต่อสิทธิเสรีภาพส่วนบุคคล	2.667	1.269	เห็นด้วยปานกลาง
6. การปิดกั้นเสรีภาพในการแสดงออกของประชาชน	2.600	1.133	เห็นด้วยปานกลาง
7. การสร้างความเชื่อมั่นในการใช้งานอินเทอร์เน็ต	3.267	0.868	เห็นด้วยปานกลาง
ผลลัพธ์ภาพรวมในทัศนะของพนักงานเจ้าหน้าที่	3.295	0.618	เห็นด้วยปานกลาง
ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐ			
1. การตระหนักในการใช้คอมพิวเตอร์	4.286	0.726	เห็นด้วยอย่างยิ่ง
2. การป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์	4.286	0.726	เห็นด้วยอย่างยิ่ง
3. การป้องกันการละเมิดสิทธิเสรีภาพในการใช้คอมพิวเตอร์ของผู้อื่น	4.000	1.109	ค่อนข้างเห็นด้วย
4. การป้องกันการทำให้ระบบคอมพิวเตอร์ของผู้อื่นเสียหาย	4.143	0.663	ค่อนข้างเห็นด้วย
5. การใช้อำนาจของพนักงานเจ้าหน้าที่ที่กระทบต่อสิทธิเสรีภาพส่วนบุคคล	3.643	1.151	ค่อนข้างเห็นด้วย

6. การปิดกั้นเสรีภาพในการแสดงออกของประชาชน	3.500	1.092	ค่อนข้างเห็นด้วย
7. การสร้างความเชื่อมั่นในการใช้งานอินเทอร์เน็ต	3.571	0.756	ค่อนข้างเห็นด้วย
ผลลัพธ์ภาพรวมในทัศนะของผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐ	3.918	0.475	ค่อนข้างเห็นด้วย
ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน			
1. การตระหนักในการใช้คอมพิวเตอร์	3.446	1.190	ค่อนข้างเห็นด้วย
2. การป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์	3.179	1.029	เห็นด้วยปานกลาง
3. การป้องกันการละเมิดสิทธิเสรีภาพในการใช้คอมพิวเตอร์ของผู้อื่น	3.196	0.923	เห็นด้วยปานกลาง
4. การป้องกันการทำให้ระบบคอมพิวเตอร์ของผู้อื่นเสียหาย	3.304	0.913	เห็นด้วยปานกลาง
5. การใช้อำนาจของพนักงานเจ้าหน้าที่ที่กระทบต่อสิทธิเสรีภาพส่วนบุคคล	3.375	0.983	เห็นด้วยปานกลาง
6. การปิดกั้นเสรีภาพในการแสดงออกของประชาชน	3.375	0.926	เห็นด้วยปานกลาง
7. การสร้างความเชื่อมั่นในการใช้งานอินเทอร์เน็ต	3.089	1.049	เห็นด้วยปานกลาง
ผลลัพธ์ภาพรวมในทัศนะของผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน	3.281	0.602	เห็นด้วยปานกลาง

จากตารางที่ 1 พบว่า (1) พนักงานเจ้าหน้าที่ในภาพรวม เห็นด้วยปานกลางกับผลลัพธ์ที่เกิดขึ้นจากการนำกฎหมายไปปฏิบัติ ส่วนในรายละเอียดนั้น ประเด็นที่เห็นด้วยอย่างยิ่งว่า เมื่อนำกฎหมายไปปฏิบัติแล้วได้ผลดี ได้แก่ การตระหนักและระมัดระวังในการใช้คอมพิวเตอร์ ส่วนที่ค่อนข้างเห็นด้วย คือ การป้องกันและปราบปรามการก่ออาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

(2) ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐในภาพรวม ค่อนข้างเห็นด้วยกับผลลัพธ์ที่เกิดขึ้นจากการนำกฎหมายไปปฏิบัติ ส่วนในรายละเอียดนั้น ประเด็นที่เห็นด้วยอย่างยิ่งว่า เมื่อนำกฎหมายไปปฏิบัติแล้วได้ผลดี ได้แก่ การตระหนักและระมัดระวังในการใช้คอมพิวเตอร์ และการป้องกันและปราบปรามการก่ออาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

(3) ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชนในภาพรวม เห็นด้วยปานกลางกับผลลัพธ์ที่เกิดขึ้นจากการนำกฎหมายไปปฏิบัติ ส่วนในรายละเอียดนั้น ประเด็นที่ค่อนข้างเห็นด้วยว่า เมื่อนำกฎหมายไปปฏิบัติแล้วได้ผลดี ได้แก่ การตระหนักและระมัดระวังในการใช้คอมพิวเตอร์

สมมติฐานที่ 2 พนักงานเจ้าหน้าที่ ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐ และผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน มีทัศนะแตกต่างกันในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ

ตารางที่ 2 การเปรียบเทียบทัศนะระหว่างกลุ่มในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ

แหล่งของความแปรปรวน	ผลรวมกำลังสอง	องศาของความเป็นอิสระ	ผลรวมกำลังสองเฉลี่ย	ค่าทดสอบ F	ระดับนัยสำคัญ
ระหว่างกลุ่ม	4.823	2	2.412	6.900	0.002
ภายในกลุ่ม	33.903	97	0.350		
รวม	38.726	99			

จากตารางที่ 2 พบว่า มีทัศนะที่แตกต่างกันระหว่างกลุ่มในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ ที่นัยสำคัญทางสถิติระดับ 0.05

เมื่อควบคุมอายุและประสบการณ์ในการปฏิบัติงานเกี่ยวกับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ผลการทดสอบสมมติฐานที่ 2 มีดังนี้

ตารางที่ 3 การเปรียบเทียบทัศนะระหว่างกลุ่มในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ เมื่อควบคุมอายุและประสบการณ์ในการปฏิบัติงาน

แหล่งของความแปรปรวน	ผลรวมกำลังสองประเภท III	องศาของความเป็นอิสระ	ผลรวมกำลังสองเฉลี่ย	ค่าทดสอบ F	ระดับนัยสำคัญ
รูปแบบที่ปรับ (Corrected Model)	5.377	4	1.344	3.829	0.006
จุดตัด (Intercept)	75.979	1	75.979	216.442	0.000
อายุ	0.209	1	0.209	0.594	0.443
ประสบการณ์ในการปฏิบัติงาน	0.296	1	0.296	0.844	0.360
สถานภาพ	4.153	2	2.077	5.916	0.004
ความคลาดเคลื่อน	33.349	95	0.351		
ผลรวม	1177.306	100			
ผลรวมที่ปรับ (Corrected Total)	38.726	99			

จากตารางที่ 3 เมื่อควบคุมอายุและประสบการณ์ในการปฏิบัติงาน พบว่า มีทัศนะที่แตกต่างกันระหว่างกลุ่มในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ ที่นัยสำคัญทางสถิติระดับ 0.05

ผลการทดสอบคู่แตกต่างโดยใช้ Least Significant Difference มีดังนี้

ตารางที่ 4 การทดสอบคู่แตกต่างในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ เมื่อควบคุมอายุและประสบการณ์ในการปฏิบัติงาน

กลุ่ม(I)	กลุ่ม(J)	(I-J)	ระดับนัยสำคัญ
พนักงานเจ้าหน้าที่	ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐ	-0.684(*)	0.003
	ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน	-0.077	0.647
ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐ	พนักงานเจ้าหน้าที่	0.684(*)	0.003
	ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน	0.608(*)	0.001
ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน	พนักงานเจ้าหน้าที่	0.077	0.647
	ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐ	-0.608(*)	0.001

จากตารางที่ 4 พบว่า ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐมีทัศนะในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติ แตกต่างจากทั้งเจ้าพนักงานของรัฐและผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน ที่นัยสำคัญทางสถิติระดับ 0.05

สมมติฐานที่ 3 เจตนารมณ์ของกฎหมาย โครงสร้างของหน่วยงานตามกฎหมาย มาตรฐานของกฎหมาย คุณสมบัติของผู้ปฏิบัติงาน การประสานงาน ความชัดเจนของกฎหมาย พฤติกรรมของผู้ปฏิบัติงาน และเงื่อนไขทางเศรษฐกิจ สังคมและการเมือง มีอิทธิพลต่อผลลัพธ์จากการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ

ตารางที่ 5 ปัจจัยที่มีอิทธิพลต่อการนำกฎหมายไปปฏิบัติ

รูปแบบ	ค่าสัมประสิทธิ์ที่ไม่ได้ปรับ	ความคลาดเคลื่อนมาตรฐาน	ค่าสัมประสิทธิ์มาตรฐาน	ค่าทดสอบ t	ระดับนัยสำคัญ
ค่าคงที่	2.116	0.388	–	5.454	0.000
พฤติกรรมของผู้ปฏิบัติงาน	0.543	0.106	0.482	5.143	0.000
โครงสร้างของหน่วยงานตามกฎหมาย	0.160	0.072	0.208	2.223	0.029

R^2= 0.218 F = 13.521 Sig. F = 0.000

ผลการวิเคราะห์พบว่า พฤติกรรมของผู้ปฏิบัติงานมีอิทธิพลต่อการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ มากที่สุด รองลงไป ได้แก่โครงสร้างของหน่วยงานตามกฎหมาย อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยสามารถอธิบายความสำเร็จของการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ ได้ร้อยละ 21.80

สรุปผล

ผลการวิจัยการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ พบว่า ได้ผลในระดับปานกลาง โดยผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐมีทัศนะในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติแตกต่างจากทั้งพนักงานเจ้าหน้าที่ของรัฐและผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน และปัจจัยที่มีอิทธิพลต่อการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ ได้แก่ พฤติกรรมของผู้ปฏิบัติงานและโครงสร้าง ของหน่วยงานตามกฎหมาย

อภิปรายผล

เหตุที่การนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไปปฏิบัติ ได้ผลปานในระดับกลาง เนื่องมาจากกฎหมายฉบับนี้ถูกนำมาใช้เป็นเครื่องมือทางการเมืองมากกว่าที่จะนำมาใช้เพื่อการป้องกันและปราบปราม การก่ออาชญากรรมคอมพิวเตอร์ ไม่ว่าจะเป็นรัฐบาลที่มาจากการเลือกตั้งชุดที่นายอภิสิทธิ์ เวชชาชีวะ และนางสาวยิ่งลักษณ์ ชินวัตร เป็นนายกรัฐมนตรี หรือรัฐบาลที่มาจากการทำรัฐประหารเมื่อปี 2557 โดยมีพลเอกประยุทธ์ จันทร์โอชา เป็นหัวหน้าคณะรักษาความสงบแห่งชาติและนายกรัฐมนตรี คดีที่เกิดขึ้นโดยอาศัยข้อหาตามกฎหมายดังกล่าวส่วนใหญ่จะเกี่ยวข้องกับการเผยแพร่เนื้อหาในอินเทอร์เน็ต ไม่ใช่เป็นคดีอาชญากรรมคอมพิวเตอร์ที่แท้จริงแต่อย่างใด และบุคคลที่ตกเป็นผู้ต้องหาจำนวนไม่น้อยจะเป็นผู้ให้บริการที่ไม่ได้โพสต์ข้อมูลด้วยตนเอง โดยเฉพาะในช่วงรัฐประหาร

รัฐบาลได้เจรจากับผู้ให้บริการรายใหญ่ระดับโลก อาทิ Google, YouTube และ Facebook เพื่อ “ขอความร่วมมือ” ให้ระงับการเข้าถึงเว็บไซต์จากผู้ชมในประเทศไทย นอกจากนี้ กองทัพบกได้จัดตั้งศูนย์ไซเบอร์กองทัพบกเพื่อเฝ้าระวังและติดตามข้อมูลข่าวสารที่บิดเบือน โจมตี ใส่ร้าย และละเมิดสถาบันผ่านเว็บไซต์และสื่อสังคมออนไลน์ และได้ปิดเว็บไซต์เหล่านี้อย่างต่อเนื่อง ซึ่งการกระทำที่ไม่ตรงกับเจตนารมณ์ของกฎหมายได้สร้างความวิตกกังวล และมีผลกระทบในทางลบต่อเสรีภาพในการแสดงออกในโลกไซเบอร์อย่างมาก

เหตุที่ผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐมีทัศนะในเรื่องของผลลัพธ์จากการนำกฎหมายไปปฏิบัติแตกต่างจากทั้งพนักงานเจ้าหน้าที่และผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชน เพราะผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาครัฐมีสถานภาพก้ำกึ่งระหว่างการเป็นพนักงานเจ้าหน้าที่และการเป็นผู้ดำเนินการอินเทอร์เน็ตในหน่วยงานภาคเอกชนในแง่ของการเป็นพนักงานเจ้าหน้าที่ จะเห็นด้วยว่า กฎหมายฉบับนี้ก่อให้เกิดผลดีในแง่ของการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ ทำให้ประชาชนตระหนักและมีความเชื่อมั่นในการใช้คอมพิวเตอร์ แต่ในแง่ของการเป็นผู้ดำเนินการอินเทอร์เน็ตในลักษณะคล้ายคลึงกับหน่วยงานภาคเอกชน จะเห็นด้วยว่า กฎหมายฉบับนี้ยังมีการปิดกั้นเสรีภาพในการแสดงออก รวมทั้งการใช้อำนาจของพนักงานเจ้าหน้าที่มีผลกระทบต่อสิทธิเสรีภาพส่วนบุคคลค่อนข้างมาก

เหตุที่พฤติกรรมของผู้ปฏิบัติงาน และโครงสร้างของหน่วยงานตามกฎหมายมีอิทธิพลต่อการนำกฎหมายไปปฏิบัติจะเป็นไปตามหลัก Weberian Bureaucracy กล่าวคือ โครงสร้างของหน่วยราชการมีการแบ่งงานกันทำอย่างเป็นทางการตามกฎหมาย ข้าราชการจะยึดความมีเหตุมีผลและมุ่งปฏิบัติตามกฎเกณฑ์ที่กำหนดไว้ตามกรอบของระเบียบแบบแผนที่เป็นทางการและเป็นลายลักษณ์อักษรของหน่วยราชการ ทำให้พฤติกรรมของข้าราชการขาดความยืดหยุ่น ต้องทำตามขั้นตอนและกฎเกณฑ์ต่าง ๆ อย่างเคร่งครัด ซึ่งส่งผลทำให้ข้าราชการมีทัศนะว่า กฎหมายคือ เป้าหมายขององค์การ ดังนั้น การปฏิบัติงานของข้าราชการจึงให้ความสำคัญต่อกฎหมายมากกว่าการบริการประชาชน ดังจะเห็นได้จากความผิดตามมาตรา 14-16 ของ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น ถือเป็นการกระทำอาชญากรรมที่มีประมวลกฎหมายอาญารองรับอยู่แล้ว ซึ่งความผิดประเภทนี้ ได้สร้างความขัดแย้งและถูกวิพากษ์วิจารณ์มากที่สุด เพราะพนักงานเจ้าหน้าที่มักจะใช้เป็นข้อหาเพื่อปิดกั้นเว็บไซต์ รวมไปถึงการดำเนินคดีกับทั้งผู้ใช้และผู้ให้บริการอินเทอร์เน็ตตามประมวลกฎหมายอาญาด้วย ซึ่งไม่เกี่ยวข้องกับความผิดโดยเนื้อหาที่ถูกนำเข้าด้วยคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แต่อย่างใด

ข้อเสนอแนะ

1. ข้อเสนอแนะทางกฎหมาย จะมีดังนี้

1.1 พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ควรใช้กับความผิดที่ผู้กระทำมุ่งก่ออาชญากรรมต่อ "ระบบหรือข้อมูลคอมพิวเตอร์" โดยตรงเท่านั้น ไม่นำไปใช้กับการก่ออาชญากรรมทั่วไป (ลักทรัพย์ ยักยอกทรัพย์ ฯลฯ) ทั้งนี้เพราะมีประมวลกฎหมายอาญาบังคับใช้อยู่แล้ว

1.2 แก้ไขเนื้อหาในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฉบับปัจจุบันให้มีความชัดเจน ดังนี้

1.2.1 แก้ไขมาตรา 14 (1) (การนำข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมหรือเท็จเข้าสู่ระบบคอมพิวเตอร์โดยทุจริตหรือโดยหลอกลวง ที่น่าจะเกิดความเสียหายแก่ประชาชน) และมาตรา 14 (2) (การนำข้อมูลคอมพิวเตอร์ที่เป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน) เพื่อเอาผิดเฉพาะเรื่อง Phishing และนิยามคำศัพท์ต่าง ๆ ในมาตรา 14 (2) ได้แก่ “ความมั่นคงปลอดภัยของประเทศ” “ความปลอดภัยสาธารณะ” “ความมั่นคงในทางเศรษฐกิจของประเทศ” และ “โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ” ให้มีความชัดเจนแน่นอน ทั้งนี้เพื่อป้องกันหรือลดผลกระทบอันจะเกิดขึ้นจากการบังคับใช้กฎหมายหรือการนำกฎหมายไปใช้ในทางที่มิชอบ

1.2.2 นำหลักการ “แจ้งเตือนและแจ้งเตือน” (Notice and Notice) มาใช้สำหรับการแจ้งเตือน การระงับและการนำข้อมูลออกจากระบบ แทนหลักการ “แจ้งเตือนและลบออก” (Notice and Takedown) เพราะจะเหมาะสมกับยุคสมัยของ User-generated content ในปัจจุบันมากกว่า

1.2.3 จำกัดอำนาจของรัฐมนตรีในการออกประกาศ ถ้าไม่กระทบต่อสิทธิเสรีภาพของประชาชน รัฐมนตรีสามารถออกได้ด้วยตนเอง แต่ถ้ามีผลกระทบต่อสิทธิเสรีภาพของประชาชน อาทิ การระงับการเข้าถึงข้อมูล การเปิดเผยตัวตน ฯลฯ ต้องให้สภาเป็นผู้พิจารณา

1.2.4 กำหนดคุณสมบัติของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ที่มาจากการแต่งตั้งของรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมให้ชัดเจน เพราะมาตรา 20 วรรคสาม ระบุไว้เพียงว่า คณะกรรมการฯ แต่ละคณะ ให้มี 9 คน โดย 3 ใน 9 ให้มาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง ในลักษณะลอย ๆ เท่านั้น

1.2.5 เพื่อให้กฎหมายมีความเที่ยงธรรม และทันต่อการเปลี่ยนแปลงของเทคโนโลยี ให้นำหลักการและกฎหมายต่อไปนี้ มาใช้เป็นแนวทางสำหรับการปรับปรุงแก้ไขให้ทันสมัยและทันกาลอยู่เสมอ ได้แก่ (1) พระราชกฤษฎีกาการทบทวน ความเหมาะสมของกฎหมาย พ.ศ. 2558 (2) The International Principles on the Application of Human Rights to Communications Surveillance และ (3) Manila Principles on Intermediary Liability

1.2.6 นิยาม “ข้อมูลคอมพิวเตอร์” ตามมาตรา 3 ได้ผนวกข้อมูลการสื่อสารทั้ง 2 ประเภท คือ เฉพาะคอมพิวเตอร์ (อาทิ โปรแกรม รหัส) และเฉพาะมนุษย์ (อาทิ ภาษา ภาพ เสียง) เข้ามาอยู่ด้วยกัน กรณีนี้ทำให้เกิดปัญหาในการดำเนินคดีความขึ้น เพราะได้มีการนำ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ไปใช้ในการดำเนินคดีเกี่ยวกับ “ข้อมูลคอมพิวเตอร์” ทั้ง 2 ประเภท ตามประมวลกฎหมายอาญา ซึ่งถือว่าไม่สมเหตุสมผล จึงควรแก้ไขให้ถูกต้องและชัดเจน

2. ข้อเสนอแนะทางนโยบาย จะมีดังนี้

2.1 จัดตั้งศาลชำนัญพิเศษเพื่อพิจารณาคดีที่เกี่ยวกับคอมพิวเตอร์โดยเฉพาะ ดั่งศาลชำนาญพิเศษที่มีการจัดตั้งแล้ว อาทิ ศาลแรงงาน ศาลภาษีอากร ศาลเยาวชนและครอบครัว

2.2 พนักงานเจ้าหน้าที่จำนวนมากที่ได้รับการแต่งตั้งให้ปฏิบัติหน้าที่ตามหมวด 2 ของกฎหมาย ไม่ได้เป็นผู้มีคุณสมบัติตามหลักเกณฑ์ในกฎหมาย ดังนั้น จึงให้มีการแก้ไขหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตาม

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้ชัดเจนและเข้มงวดเป็นพิเศษ ไม่ให้มีการยกเว้นคุณสมบัติใด ๆ เกิดขึ้นเพื่อป้องกันปัญหาที่จะเกิดตามมา

ประโยชน์ที่ได้รับจากการวิจัย

1. นำไปใช้กำหนดนโยบายและมาตรการที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

2. นำไปใช้แก้ไข พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือการแก้ไขกฎหมายที่เกี่ยวข้องอื่น ๆ เพื่อให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป

References

Barrett, S., & Fudge, C. (Eds.). (1981). *Policy and action*. London: Meuthuen.

Ben–Zadok, E. (2006). Solid theory and soft implementation in policy design: Florida compact development policies. *International Planning Studies*, 11(1), 59–81.

Brenner, S. W. (2012). *Cybercrime and the law: challenges, issues, and outcomes.* Boston: Northeastern University Press.

Butler, M. J. R. (2003). Managing from the inside out: Drawing on 'receptivity' to explain variation in strategy Implementation. [Special Issue], *British Journal of Management*, 14, S47–S60.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A Routine activity approach. *American Sociological Review.* 44(4), 588–608.

Edwards, G. C. III. (1980). Implementing public policy. Washington, DC: Congressional Quarterly.

Goggin, M. L., Bowman, A. O., Lester, J. P., & O'Toole, L. J., Jr. (1990). *Implementation theory and practice: Toward a third generation.* Glenview, IL: Scott, Foreman/ Little, Brown.

Hill, J. B., & Marion, N. E. (2016). *Introduction to cybercrime: Computer crimes, laws, and policing in the 21st century.* Santa Barbara, CA: Praeger.

Hirschi, T. (1969). *Causes of delinquency*. University of California Press.

Jaishankar, K. (2008). Space Transition Theory of cyber crimes. In Schmallager, F., & Pittaro, M. (Eds.), *Crimes of the Internet* (pp. 283–301). Upper Saddle River, NJ: Prentice Hall.

Lertkitikul, P. (2007). *The Computer–Related Crime Act 2007: A case study of criminal liability in access to computer system and computer data.* Bangkok: Chulalongkorn University.

Mazmanian, D., & Sabatier, P. A. (1983). *Implementation and public policy*. Glenview, Ill.: Scott, Foresman.

Moore, R. (2005). *Cybercrime: Investigating high–technology computer crime*. Cleveland, MS: Anderson Publishing.

Nakamura, R. T., & Smallwood, F. (1980). *The politics of policy implementation*. New York: St. Martin's.

Napibul, A. (2008). *Problems and obstacles of the enforcement of the Computer Crime Act B.E. 2550.* Bangkok:

Chulalongkorn University.

Onpueng, S. (2011). *The enforcement of computer related crime act B.E. 2007: a case study of offence relating to dissemination of information regarding the security of the Kingdom.* Bangkok: Chulalongkorn University.

Parker, S. N., & Oüra, S. S. (1973). *Computer abuse.* Menlo Park, CA: Stanford Research Institute.

Pressman, J. L. & Wildavsky, A. (1973). *Implementation*. Berkeley: University of California Press.

Ryan, N. (1996). Some advantages of an integrated approach to implementation analysis: A study of Australian industry policy. *Public Administration*, 74, 737–753.

Sabatier, P. A. (1991). Towards better theories of the policy process. *Political Science and Politics*, 24(2), 147–156.

Sakdulyatham, S. (2008). *Knowledge, impact assessment and behavior tendency of internet users about the Computer Crime Act B.E. 2550.* Bangkok: Chulalongkorn University.

Schofield, J. (2001). Time for revival? Public policy implementation: A review of the literature and an agenda for future research. *International Journal of Public Administration*, 3(3), 245–263.

Terpstra, J., & Havinga, T. (2001). Implementation between tradition and management: Structuration and styles of implementation. *Law and Policy*, 23(1), 95–116.

Van Meter, Donald S., & Van Horn, Carl E. (1975). The policy implementation process: A conceptual framework. *Administration & Society*, 6(4), 445–488.

Vangen, Siv., & Huxam, Chris. (2003). Enacting leadership for collaborative advantage: Dilemmas of ideology and pragmatism in the activities of partnership managers. *British Journal of Management*, 14, S61–S76.